Topics:

security organization [2], data owner [3], business owner [4]

Information Security Management Organization [1]

SS-08-006 Information Security Management Organization

Issue Date: 3/31/2008

Revision Effective Date: 3/31/2008

PURPOSE

In compliance with the Enterprise Information Security Charter P-07-005.01, each agency must implement a formal internal information security program. Agency executive management is ultimately responsible for protecting agency-wide assets and setting security philosophy that will determine the overall effectiveness of the information security program. As such, it is necessary to establish a security management organization with clearly defined roles and responsibilities that will collectively and cooperatively develop, implement, and maintain the agency?s information security program by aligning security objectives with the business objectives of the organization.

This standard establishes the minimum elements of an information security management organization.

STANDARD

Each agency?s information security infrastructure shall have a security management organization that oversees the security program, establishes and periodically reviews security controls, and authorizes systems to operate. Agency heads shall ensure the appropriate officials and personnel are assigned the following minimum security roles and responsibilities.

- Agency head or other executive management (ex. CIO) shall be ultimately responsible for the security of information assets held by the agency and assign personnel to the appropriate security roles.
- Business/Information System Owner shall establish the strategic objectives for the applications and technology that support their business functions.
- Data/Information Owner shall define the controls necessary to protect the data within their business function and shall knowingly accept the risks associated with operating an information system processing that data.
- Information System Security Officer (ISSO) shall administer the information security program. The ISO shall be the primary point of contact to the State Chief Information Security Officer (CISO) on security matters for the agency.
- Business Continuity Coordinator shall ensure a process exists to maintain continuous operations of critical functions during a crisis or to recover critical functions within established Recovery Time Objectives (RTO).

GUIDELINES

These are security responsibilities and do not mandate the need for a full-time security staff, employees or positions. Smaller agencies and agencies with small IT budgets may chose to assign these functions as additional duties, or all of these functions may be the responsibility of one or two individuals. What is important is that agency management take ownership for the security of their information assets, and ensure that whoever is assigned these security functions, understands their responsibilities and is able to fulfill their role.

Agency heads whose IT infrastructure is managed by a separate agency or service provider are still responsible for the